UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,583	02/12/2002	Carl Young	G08.015	6976

28062 7590 02/08/2007

BUCKLEY, MASCHOFF, TALWALKAR LLC
50 LOCUSTAVENUE
NEW CANAAN, CT 06840

EXAMINER	
RAHMAN, FAHMIDA	
ART UNIT	PAPER NUMBER
2116	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/074,583	YOUNG, CARL	
	Examiner	Art Unit	
	Fahmida Rahman	2116	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to communications filed on 11/24/06.

2. Claims 1, 13, 17, 18, 22 and 24 have been amended, claims 25-28 have been cancelled and no new claims have been added. Thus, claims 1-24 are pending.

Claim Objections

Claim 19 is objected to because of the following informalities: claim 19 recites "a first variable" and "a second variable" in lines 2-3. It is not clear whether they are same or different from "first set of risk variables" and "second set of risk variables" defined in line 5 and line 7 of claim 1. For the rest of the action, it is assumed that first and second variable are from either first set of risk variables or second set of risk variables.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 1-9, 15-18, 20, 22-24 are rejected under 102(e) as being anticipated by Townsend (US Patent Application Publication 2002/0188861).

For claim 1, Townsend teaches a computer implemented method for managing risk related to a security risk event (Fig 1), the method comprising:

- **receiving formation** (105; [0027]) **relating to a particular security risk event** (Fig 3A and Fig 3B show the attack types Tj, which is the particular security risk event. The information relating Tj is received in 110);
- **automatically processing, by a computer, the information received to associate the received information with a first set of risk variables** (the first set of risk variables are "Policy Awareness" and "Policy Compliance" as shown in Fig 4) **related to the particular security risk event** (these variables are related to countermeasures as shown in Fig 3B, which in turn are related to attacks, or the particular security risk event);
- **defining a second set of risk variables** ("corporate security awareness", "Unique training" shown in Fig 4) **related to the particular security risk event** ("corporate security awareness", "Unique training" shown in Fig 4, are related to attacks or particular security event as shown in Fig 3B), **wherein the first set of risk variables and the second set of risk variables are different** (first set of risk variables, "Policy awareness" and "Policy Compliance" are different from second set of risk variables, "Corporate security awareness", "Unique training", "Training Compliance");

- **associating a portion of the received information related to the particular security risk event and not associated with the first set of risk variables with the second set of risk variables** (the information related to "Training 2.0" in Fig 2 is associated with second set of risk variables, but not associated with first set of risk variables as shown in Fig 4); and
- **and calculating a security level** (170) **using the processed information and a set of relationships established between the first set and second set of risk variables** (115, 120, 130, 135, 140, 150, 155 show how the security level is calculated using the processed information and the relationship between risk variables).

For claims 2 and 3, note [0048] of page 4, which mentions that conformance value quantifies the amount of risk and the difference between current security policy/best practice security policy.

For claim 4, [0048] mentions that total amount of risk to the organization may be estimated.

For claim 5, b in [0047] is the recommended effectiveness level.

For claim 6, 145 provides the suggestion or recommendation.

For claim 7, the information, security level and suggested security measure are stored as they are necessary in intermediate steps to perform 180.

For claim 8, 180 in Fig 1 shows the generation of diligence report.

For claim 9, Fig 6 shows the report, which comprises inquiries made ("no specific training identified") and security measures executed ("courses available").

For claim 15, [0037] mentions about the classification that is used in Fig 1 to calculate 170.

For claim 16, Fig 4 shows multiple levels associated with each category of risk variables.

For claim 17, aggregation is performed in [0046] and [0047].

For claim 18, Fig 4 shows how the risk variables are affecting each other.

For claim 20, 170 is recalculated for next application as shown in Fig 1.

For claims 22, Townsend teaches the following limitations:

A computerized system for managing risk related to a particular security risk event (Fig 1-7), **the system comprising**:

- **a computer server** (730) **accessible with a system access device** (700, 724) **via a communications network** (726, 728, 722);

  and executable software stored on the server and executable on demand ([0061] of page 5), **the software operative with the server to cause the system to:**

- **receiving formation** (105; [0027]) **relating to a particular security risk event** (Fig 3A and Fig 3B show the attack types Tj, which is the particular security risk event. The information relating Tj is received in 110);

- **automatically processing, by a computer, the information received to associate the received information with a first set of risk variables** (the first set of risk variables are "Policy Awareness" and "Policy Compliance" as shown in Fig 4) **related to the particular security risk event** (these variables are related to countermeasures as shown in Fig 3B, which in turn are related to attacks, or the particular security risk event);

- **defining a second set of risk variables** ("corporate security awareness", "Unique training" shown in Fig 4) **related to the particular security risk event** ("corporate security awareness", "Unique training" shown in Fig 4, are related to attacks or particular security event as shown in Fig 3B), **wherein the first set of risk variables and the second set of risk variables are different** (first set of risk variables, "Policy awareness" and "Policy

Compliance" are different from second set of risk variables, "Corporate security awareness", "Unique training", "Training Compliance");

- **associating a portion of the received information related to the particular security risk event and not associated with the first set of risk variables with the second set of risk variables** (the information related to "Training 2.0" in Fig 2 is associated with second set of risk variables, but not associated with first set of risk variables as shown in Fig 4); and
- **and calculating a security level** (170) **using the processed information and a set of relationships established between the first set and second set of risk variables** (115, 120, 130, 135, 140, 150, 155 show how the security level is calculated using the processed information and the relationship between risk variables).

For claim 23, the system of Towsend uses software to calculate security level. Thus, the software tool has to be feed with the information as shown in Fig 2 by an electronic means, since computer itself is an electronic device.

For claim 24, the system of Towsend must have the corresponding instruction code, medium and data signal to implement the system of claim 22.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 10-14, 19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Townsend (US Patent Application Publication 2002/0188861), Teller-Kanzler et al (EP 0999489 A2).

For claims 10-13, Townsend does not teach that the suggested security measure comprises physical protection. Teller-Kanzler et al teach physical protection as explained below for claims 10-13.

For claim 10, note cell 11 of level 4 in Fig 3, which mentions that the determination of level of protection required for information assets is made. Thus, the suggested security measure comprises physical protection of media containing information relating to the transaction.

For claim 11, Teller-Kanzler et al teach that the suggested security measure comprises physical protection of a facility. Note the cell 5 of level 5 in Fig 4, which mention about full integration between physical security and information security. Thus, the suggested

security measure comprises physical protection of a facility associated with the security risk.

For claim 12, cell 12 of level 5 in Fig 4 mentions about organization wide dissemination of security alerts, which is a physical protection of a building. Thus, the suggested security measure comprises physical protection of a building associated with a business transaction.

For claim 13, note cells 3 and 4 of level 5 in Fig 5, which mention that the help desk and organization wide reporting of security incidents. Thus, the suggested action comprises notifying an authority regarding potential breach of security.

It would have been obvious for an ordinary skill in the art at the time the invention was made to combine the teachings of Townsend and Teller-Kanzler et al. One ordinary skill would be motivated to incorporate physical security in the system, as that strengthens the existing security.

For claim 14, Townsend does not teach branding the suggested security measure according to the set of relationships between the risk variables. Teller-Kanzler et al teach branding the suggested security measure according to the set of relationships between the risk variables. Note, lines 16-18 of column 12 mention that the score is used to determine if the organization can move from one level to next level. Thus, the

score is an indicative of suggested security measure, which is a set of relationships between variables defined in ISEM grid. One ordinary skill would be motivated to brand the suggested security according to the set of relationships between the risk variables, since that would provide the information how the suggested security can be achieved.

For claim 19, Townsend does not teach how data including first variable can affect a weighting for a second variable. Teller-Kanzler et al teach how data including first variable can affect a weighting for a second variable. Note line 22 of column 12, which mentions about the use of decision tree, a relationship algorithm. In addition, lines 12-16 of column 12 mention about the weighting of cells according to importance. The decision tree structure defines the relationship among variables, including the weighting. Thus, the calculation comprises a relationship algorithm that determines how first variable effect weighting of other variables. One ordinary skill would be motivated to incorporate the relationship algorithm within the calculation about how data including first variable can affect a weighting for a second variable, as such interrelationship provides better calculation of security level.

For claim 21, Teller-Kanzler et al or Townsend do not explicitly teach teach recalculation of security level responsive to progression of chronology. However, lines 13-16 of column 14 of Teller-Kanzler et al mention that the various modifications would be apparent to ordinary skill in the art and the disclosure is intended to cover all such modifications.

In addition, [0049] of column 12 of Teller-Kanzler et al mentions that the managers use the score to determine whether they are satisfied with the level of organization in light of risk. Since, the new information or chronology of events may change the security level of the organization, recalculation is necessary to obtain the correct level of the organization in light of risk.

One ordinary skill in the art would have been motivated to recalculate the security level responsive to new information and/or progression of chronology of events in the system of Townsend and Teller-Kanzler et al, since these events/information may make the change of score of the security level. In that case, management may feel that the existing level calculated by the method is not a proper reflection of security model in light of new information or progressive chronology of events. They may want to verify that the new set of received information/progressive events still verifies the security level of the entity by recalculating the security level in receipt of new information.

Response to Arguments

Applicant's arguments filed on 11/24/2006 have been fully considered but they are not persuasive.

Applicant argues that Townsend does not teach the limitations "defining a second set of risk variables related to the particular security risk event, wherein the first set of risk

variables and the second set of risk variables are different; associating a portion of the received information related to the particular security risk event and not associated with the first set of risk variables with the second set of risk variables".

Examiner disagrees. Townsend teaches defining a second set of risk variables ("corporate security awareness", "Unique training" shown in Fig 4) related to the particular security risk event ("corporate security awareness", "Unique training" shown in Fig 4, are related to attacks or particular security event as shown in Fig 3B), wherein the first set of risk variables and the second set of risk variables are different (first set of risk variables, "Policy awareness" and "Policy Compliance" are different from second set of risk variables, "Corporate security awareness", "Unique training", "Training Compliance") and associating a portion of the received information related to the particular security risk event and not associated with the first set of risk variables with the second set of risk variables (the information related to "Training 2.0" in Fig 2 is associated with second set of risk variables, but not associated with first set of risk variables as shown in Fig 4).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fahmida Rahman whose telephone number is 571-272-8159. The examiner can normally be reached on Monday through Friday 8:30 - 5:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Rehana Perveen can be reached on571-272-3676. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fahmida Rahman
Examiner
Art Unit 2116

THUAN N. DU
PRIMARY EXAMINER